Journal of Governance Risk Management Compliance and Sustainability (JGRCS), Vol. 6 No. 1 (2026) https://doi.org/10.31098/jgrcs.v6i1.3682

Research Paper

A Documentary-Based GRC Maturity Assessment Using OCEG Practices: Single Case of PT Kereta Api Indonesia

Canna Divertana Hernama
Program Magister Teknik Transportasi, Fakultas Teknik Sipil dan Lingkungan,
Institut Teknologi Bandung

Received: August 28, 2025	Revised : January 19, 2026	Accepted : February 20, 2026	Online : April 30, 2026

Abstract

This article assesses the maturity of PT Kereta Api Indonesia (Persero)'s Governance, Risk, and Compliance (GRC) capabilities through the lens of strategic alignment. The research uses documentary analysis of 2024 documents (Annual and Sustainability Reports, Company Profiles, and Financial Reports) mapped to 23 OCEG practices (12–7–4) with a maturity scale of 1–5. The procedure includes audit trail evidence mapping and a double scoring scheme to improve replicability. The results indicate Levels 3 to 4 in several practices: Governance (KPIs & reporting, transparency/PPID, SPI/ICS effectiveness statements), Risk (digitalized ISO 31000 cycle through SMARTKA/RCSA and its correlation with RKAP/RJPP and safety/IBPR), and Compliance (implementation of SMAP ISO 37001, WBS updates and their integration with national authorities, and compliance reporting discipline). The Strategic Alignment Model analysis indicates a Path B (Technology Transformation*)* pattern with Path D (Service Level*)* elements through the integration of GRC solutions into the performance infrastructure (KPI/ICS). This study offersa replicable GRC assessment protocol with the case of state-owned railway companies. The findings reinforce the evidence that integrated GRC can improve the total performance of public service organizations.

Keywords: *GRC, OCEG V3.5, Strategic Alignment, ISO 31000, ISO 37001, State-Owned Railway Company*.

INTRODUCTION

The state-owned railway company PT Kereta Api Indonesia (Persero) (PT KAI) operates in a VUCA (volatility, uncertainty, complexity, ambiguity) environment with increasing pressure on safety, service performance, and sustainability expectations. At the same time, functional fragmentation across organizational units often creates inconsistencies between corporate strategy, operational processes, and enabling technologies, particularly in large public-sector organizations (OCEG, 2024).

The concept of VUCA, which represents volatility, uncertainty, complexity, and ambiguity, has a significant impact on the railway business, which faces various challenges in navigating a dynamic operational landscape. This environment is influenced by various factors, such as economic instability, fuel price fluctuations, technological advances, regulatory/ policy changes, and fluctuating demand patterns (Omotayo et al., 2022; Attalansyah & Anshori, 2023), requiring strong response strategies for organizations operating in this sector. In this sector, such volatility primarily amplifies safety, compliance, and operational risk, thereby increasing the importance of integrated governance, risk management, and compliance mechanisms.

In the context of GRC (Governance-Risk-Compliance), OCEG positions GRC as an integrated capability to "achieve goals reliably, overcome uncertainty, and act with integrity" while reconnecting departments, roles, and information systems to produce a single source of truth for managerial decisions (OCEG, 2024). However, while the integrated GRC concept is well established normatively, many organizations still struggle to demonstrate—using audit-traceable

Corresponding author's email: cannadivertana@yahoo.com

evidence—how far such integration has been operationalized in practice.

In Asian countries, strong corporate governance is essential to prevent financial fraud and manage agency problems, which are important for maintaining market stability and investor confidence (Wahyuningrum et al., 2023). Risk management acts as a mediator between corporate governance and financial performance, indicating that effective risk management can improve a company's financial results by reducing potential risks (Rehman et al., 2021). The effectiveness of risk governance is influenced by external and internal demands to improve risk management processes. Organizations with formal and strategically focused risk governance processes are better prepared to deal with uncertainty (Beasley et al., 2022). Compliance with regulatory requirements, such as mandatory sustainability reporting, is enhanced by sustainable corporate governance mechanisms. These mechanisms ensure high-quality reporting and transparency, which are essential for stakeholder trust and regulatory compliance (Gerwing et al., 2022).

On the corporate side, PT KAI has standardized the Three Lines Model, updated its risk management policy based on ISO 31000, integrated risk into its RJPP/RKAP, and digitized monitoring as a basis for decision-making and sustainable value creation (PT KAI, 2024a). Despite these initiatives, PT KAI has not yet articulated a transparent and replicable method for translating documentary evidence into a coherent assessment of GRC maturity across governance, risk, and compliance domains. Effective coordination between governance functions is essential to avoid duplication of efforts and ensure comprehensive risk coverage (Bantleon et al., 2021).

In line with its sustainability mandate, PT KAI's ESG reporting is integrated into its Annual Report and refers to POJK 51/2017, SEOJK 16/2021, GRI 2021, and SDGs as a form of accountability (PT KAI, 2024a). A summary of the Company's profile and service portfolio is presented in the 2024 Company Profile (PT KAI, 2024b). These disclosures provide a formal accountability framework, yet they do not by themselves indicate the maturity or consistency of GRC practices across organizational processes.

In addition, the Annual and Sustainability Report, Company Profile, and 2024 Consolidated Financial Report describes the context of financial risks (e.g., liquidity risk) and management policies as triangulation evidence for GRC analysis (PT KAI, 2024c). In the public sector, governance features such as the size and independence of government agencies affect the quality of financial reports. High-quality financial reporting is associated with better online disclosure practices, which are crucial for accountability (Garcia-Lacalle & Torres, 2021).

The study therefore focuses on the systematic use of publicly available and audit-traceable corporate documents as the primary evidence base for assessing GRC maturity, with detailed data sources and procedures described in the methodology section.

Problem Statement

Accordingly, this applied study addresses four practical questions:

1. What is the maturity level of PT KAI's GRC practices when mapped to 23 OCEG practices using a five-level scale?
2. Which governance, risk, and compliance domains exhibit the most persistent gaps?
3. Which strategic alignment path is implied by the documented relationship between corporate strategy and GRC-related processes and systems; and
4. How a documentary evidence-mapping approach can generate replicable maturity scores.

Literature Review (very brief)

The GRC strategic alignment study maps GRC to the Strategic Alignment Model in four domains (external–internal × business–IT) through two pillars of strategic fit and functional integration (Shahim et al., 2012). This approach reduces four alignment paths (A–D) and confirms

that organizations with similar maturity can take different implementation paths depending on IT assets (Shahim et al., 2012). For operationalization, the literature distills 23 practices (12–7–4) from the OCEG maturity model and uses a five-level scale (1–5) (Shahim et al., 2012; OCEG, 2024). This structured methodology is important because it serves to monitor compliance and align risk management strategies with business objectives. Makaš emphasizes the increasing relevance of the GRC framework in promoting organizational sustainability (Makaš, 2023).

Limitations of Previous Research

Although providing a strong conceptual foundation, previous empirical evidence remains limited to two case studies in Europe/the Netherlands (utility companies and financial institutions) with a limited number of interviews; more importantly, prior studies do not sufficiently explain how strategic alignment and GRC maturity can be inferred solely from documentary, audit-traceable evidence without interactive data collection.

Research Gaps and Scientific Added Value

This study addresses the identified practice gap by proposing a documentary-based GRC maturity assessment protocol that specifies OCEG practices, evidence anchors in corporate disclosures, and a transparent scoring logic to support organizational improvement.

Research Objectives

Therefore, the study aims to apply an OCEG-based documentary assessment to PT KAI's 2024 disclosures in order to generate indicative GRC maturity scores and interpret the implied strategic alignment path for improvement prioritization.

LITERATURE REVIEW

Strategic Alignment Model (SAM) for GRC

The literature places GRC within the Strategic Alignment Model (SAM) framework, which combines two pillars of strategic fit (external-internal domain integration) and functional integration (business-IT process/architecture integration), then maps them to four domains (external-internal × business-IT) (Shahim et al., 2012). In its adaptation to GRC, the IT domain is represented as a GRC solution (GRC recording/logging system), while the business domain contains the organization's GRC structure/processes; strategic alignment is achieved by integrating business and IT strategies and their implementation (Shahim et al., 2012). (Figure 1).

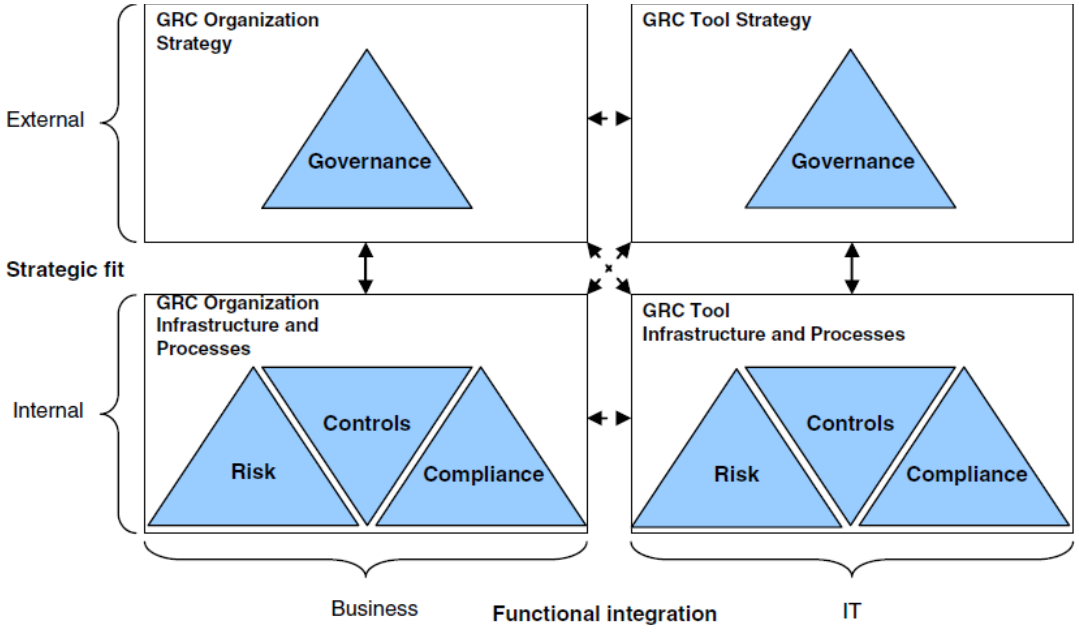

Figure 1. GRC plotted in the strategic alignment model by Henderson et al (1999); the GRCstrategic alignment model

SAM produces four GRC alignment paths (A–D): A Strategy Execution, B Technology Transformation, C Competitive Potential, D Service Level, each of which regulates the starting point (organizational strategy vs. solution strategy) and the sequence of process/technology infrastructure arrangement (Shahim et al., 2012) (Figure 2). Evidence from two case studies in the Netherlands (utility companies and financial institutions) shows that similar levels of maturity can be achieved through different paths, and that existing IT assets have a strong influence on the choiceof path (Shahim et al., 2012).

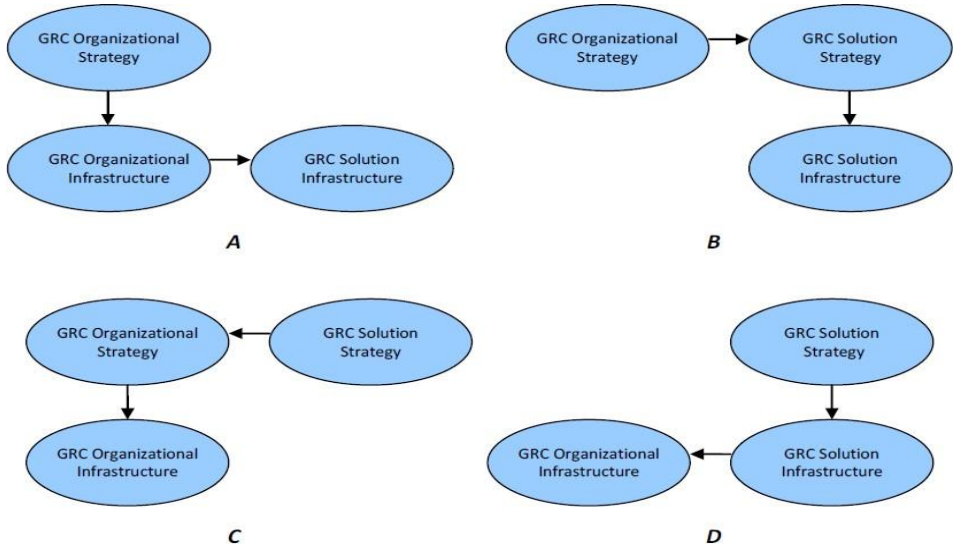

Figure. 2. Four paths to reach strategic alignment in GRC (A: Strategy execution, B: Technologytransformation, C: Competitive potential, D: Service level)

Prior studies commonly argue that integrating Governance, Risk, and Compliance (GRC) with strategic alignment models may enhance organizational performance; however, alignment is

often treated as a normative objective rather than as an empirically observable construct. The GRC framework facilitates organizations in navigating the complexity of the regulatory environment while ensuring alignment between IT and business strategies, improving the effectiveness and efficiency across processes and operations (Kurniawan et al., 2024; Vicente & Silva, 2011). (Katz et al., 2016; Imgharene et al., 2019). Various models, including SAM, emphasize alignment as a desirable organizational condition, yet provide limited guidance on how such alignment can be empirically inferred from organizational artifacts. SAM stresses the importance of achieving alignment between business and IT strategies, which is linked to improved organizational performance (Sabherwal et al., 2019; Tejada-Malaspina & Jan, 2019; Shahim et al., 2012). In most of these studies, alignment is inferred through managerial perceptions, interviews, or survey-based instruments rather than through documentary and audit-traceable evidence.

Furthermore, the concept of strategic alignment encompasses the integration of GRC principles that help organizations determine risk appetite and compliance requirements within their business strategy framework. This integration supports the alignment of technology governance with strategic business objectives, enabling companies to allocate resources efficiently and respond dynamically to market changes (Adama et al., 2024). While this holistic framing highlights the strategic intent of GRC, it does not by itself specify observable indicators that distinguish strategic alignment from mere consistency of documented practices.

In short, the application of a strategic alignment model in the context of GRC empowers organizations to create cohesive strategies that address governance, anticipate risks, and ensure compliance with strict regulations. However, without explicit analytical boundaries, such claims risk conflating strategic alignment with operational maturity or regulatory completeness.

Critical implications

First, the alignment approach shifts the GRC discussion from "tool adoption" to cross-domain strategy-process-architecture alignment. Second, the variation in paths (A–D) underscores the need for an IT-business context diagnosis before "locking in" an implementation plan. Third, maturity metrics alone are insufficient without a narrative trajectory;organizations need to evaluate fit and path-dependency when designing a GRC roadmap. In this regard, alignment in the SAM–GRC context should be interpreted as the documented coherence between strategic intent, organizational arrangements, and enabling systems, rather than as a comprehensive measure of behavioral or cultural integration.

OCEG-based GRC Practice Framework and Maturity Scale

OCEG formulates GRC as an integrated capability to "reliably achieve objectives, manage uncertainty, and act with integrity" (Principled Performance), while linking fragmented departments, roles, and skills (OCEG, 2024). For governance and assurance structures, OCEG introduces LoA/Lines of Accountability, which explain the contributions of the First–Fifth Lines to the management and assurance of performance, risk, and compliance; the arrangement of LoA is not static and must be tailored to the needs of the organization (OCEG, 2024).

The Governance, Risk, and Compliance (GRC) Capability Model is an evolving framework that integrates organizational governance practices, risk management strategies, and compliance with applicable laws and regulations. The model primarily emphasizes the institutionalization and consistency of practices, rather than the strategic alignment between governance objectives and organizational architecture. The GRC concept encompasses an integrated approach in which governance provides a framework for decision-making, risk management identifies and mitigates potential threats, and compliance ensures adherence to legaland regulatory standards.

Siahaan et al. define integrated GRC as a means for organizations to comply with anti-financial crime regulations while promoting integrity through effective leadership, risk assessment, and monitoring practices (Siahaan et al., 2022). Various authors also acknowledge the role of information systems in enhancing GRC capabilities. Wiesche et al. (2012) describe how specialized information systems help organizations navigate compliance requirements more effectively, promoting better reporting mechanisms and more efficient processes (Wiesche et al., 2011).

At the level of practice instrumentation, an alignment study (Shahim et al., 2012) distilled 23 practices from the OCEG maturity model, consisting of:

1. 12 Governance practices, namely code of conduct, strategy, organizational chart, accountabilities, meeting between accountable parties, process integration with business process, KPIs, reporting, budget, cost/benefit monitoring, transparency, and training;
2. 7 Risk practices, namely risk assessment, risk overview, risk overview containing IT risks, risk review, incident reporting, emergency process for gaps and incidents, and root cause analysis for gaps or incidents; and
3. 4 Compliance practices, namely, an overview of regulatory boundaries, an overview of internal and external rules and regulations, compliance review, and processes when confronted with non-compliance;

with a five-level GRC maturity scale, namely:

1. The practice is not available in the organization.
2. The organization is developing the practice.
3. The practice is available in the organization, but fragmented or used inconsistently throughout the organization.
4. The practice is integrated, available in the organization, and used consistently;
5. The practice is consistently measured and is undergoing improvements. based on the Capability Maturity Model (CMM) (Shahim et al., 2012).

From a synthesis perspective, three analytical implications can be drawn. First, OCEG provides a common language and accountability structure for adaptive governance and assurance. Second, the SAM–GRC framework offers a mechanism to relate these practices to cross-domain alignment paths, operationalized through the 23-practice and five-level maturity structure. Third, combining OCEG practice maturity with SAM alignment paths enables a documentary-based assessment that goes beyond compliance checklists, while remaining bound to observable organizational evidence. On the other hand, the need for cross-sector and cross-country validation remains (see 2.3).

Further Research Agenda Towards Integrated GRC

Shahim et al. (2012) emphasize two main agendas:

1. practical support for organizations that still experience GRC as separate/siloed concepts toshift to a holistic perspective, and
2. validation and enrichment of the maturity-alignment approach through additional case studies (Shahim et al., 2012).

Conceptually, OCEG positions VUCA and disconnection as "styles of disruption" that demand connected capabilities—an argument that reinforces the urgency of cross-functional GRC integration (OCEG, 2024).

The synthesis direction for this study

Building on this agenda, the synthesis direction for the present study is as follows:

1. applies SAM-GRC (A–D) to diagnose fit and trajectory in the context of state-owned railway

companies,
2. uses 23 OCEG practices (12–7–4; 1–5) as traceable measurement instruments, and
3. links the role of LoA and leading/lagging indicators to bridge the gap between governance, management, and assurance.

RESEARCH METHOD

Study design and data sources

This research uses a single-case study at PT KAI, with data sources from corporate documents for the 2024 reporting year:

1. Annual Report and Sustainability Report 2024 (policy, structure, risk management system, ICS, WBS/anti-corruption, information disclosure);
2. Consolidated Financial Report 2024 (audited); and

using the OCEG v3.5 GRC framework profile and GRC alignment articles as references for methods and instruments. To enhance methodological trustworthiness, the study applies documentary triangulation across these corporate disclosures, with each analytical claim supported by audit-traceable excerpts recorded in an evidence log that documents the source, section, and contextual interpretation of the evidence.

At PT KAI, risk management refers to ISO 31000:2018 (communication–context–assessment– mitigation–monitoring–reporting stages), organized in the Three Lines Model, integrated into RJPP/RKAP, and supported by digitalization (SMARTKA/RCSA). On the compliance side, the company operates WBS (including the integration of TPK/Corruption Crimes with the KPK/Corruption Eradication Commission) and KIP (Public Information Disclosure)/PPID policies. For financial risks, the financial statements reference market, credit, and liquidity risk management policies.

Assessment framework and instruments

The research instrument adopts a framework of 23 GRC practices (derived from the OCEG maturity model) and a 5-level maturity scale as operationalized by Shahim, Batenburg, & Vermunt (2012), consisting of:

1. 12 Governance practices, namely code of conduct, strategy, organizational chart, accountabilities, meeting between accountable parties, process integration with business process, KPIs, reporting, budget, cost/benefit monitoring, transparency, and training;
2. 7 Risk practices, namely risk assessment, risk overview, risk overview containing IT risks, risk review, incident reporting, emergency process for gaps and incidents, and root cause analysis for gaps or incidents; and
3. 4 Compliance practices, namely, an overview of regulatory boundaries, an overview of internal and external rules and regulations, compliance review, and processes when confronted with non-compliance;

with a five-level GRC maturity scoring scale, namely:

1. Level 1: The practice is not available in the organization.
2. Level 2: The organization is developing the practice;
3. Level 3: The practice is available in the organization, but fragmented or used inconsistentlythroughout the organization.
4. Level 4: The practice is integrated, available within the organization, and used consistently;
5. Level 5: The practice is consistently measured and is undergoing improvements (based on CMM).

Scoring decision rules were defined ex ante to ensure consistency. Level 3 is assigned when documentary evidence indicates the presence of a practice but shows partial coverage (limited to

specific units or subsidiaries), ad hoc or inconsistent use, or reliance on informal arrangements. Level 4 is assigned only when evidence demonstrates formal standardization (approved policies or SOPs), organization-wide applicability, and repeated use reflected in systematic reporting, system logs, or audit references. Level 5 additionally requires documented performance measurement and evidence of continuous improvement cycles.

As a theoretical foundation, the research links GRC to the Strategic Alignment Model (SAM)—two pillars of strategic fit and functional integration and four alignment paths (A–D): strategy execution, technology transformation, competitive potential, and service level. We use these paths to interpret the implications of KAI's IT architecture/capabilities on the GRC alignment path. Alignment is treated as an analytical construct inferred from the documented coherence between corporate objectives, GRC-related structures and processes, and enabling systems, rather than as a behavioral or perceptual measure.

To enrich the assessment lens, we align with OCEG v3.5: an emphasis on governance–management–assurance across performance, risk, and compliance to reliably achieve objectives, address uncertainty, and act with integrity; as well as guidance on action and control design/execution (DESIGN/PERFORM), including cross-Line of Accountability allocation and key indicator development.

Procedures for collecting and mapping evidence (*documentary analysis and evidence mapping*)

Evidence collection and mapping followed a structured documentary analysis procedure. Searching documents in the relevant sections of the 2024 KAI document (e.g., MR (Risk Management) policies/structure, integration into planning, SMARTKA/RCSA digitization; ICS; WBS; KIP/PPID; training programs). Mapping to 23 practices with evidence paired with related practices (e.g., risk assessment with ISO 31000 stages; transparency with KIP/PPID; incident reporting with WBS). Examples that serve as anchors for mapping include: ISO 31000 stages; *Three Lines* structure; RJPP/RKAP integration and SMARTKA/RCSA digitization; statistics and WBS- TPK integration; information disclosure policy; and market/credit/liquidity risk policy.

A practice was scored only when at least one primary excerpt explicitly supported its existence. Higher maturity levels require corroborating evidence, such as cross-references across different documents, repeated disclosures across sections, or system-generated records and audit findings.

Ethical considerations

This study uses public/audit-traceable corporate documents without individual data; it does not involve human subjects. Accordingly, the analysis assesses the institutionalization of GRC practices as documented in formal disclosures and does not claim effectiveness beyond what is supported by documentary evidence. When conflicting evidence was identified (e.g., formal policy claims not matched by implementation signals), the study applied a "lowest defensible score" principle. Priority was given to audited disclosures, formally issued policies or SOPs, and quantified system or audit evidence.

FINDINGS AND DISCUSSION

Summary of findings on the maturity of 23 practices (G–R–C)

In general, most GRC practices at PT KAI have been documented and operationalized, with notable strengthening in KPIs and reporting, ISO-based risk management on 31000 digitalization (SMARTKA), and integrity and transparency mechanisms (WBS and PPID), with the following details:

1. Governance. The Board of Directors' KPIs (collective and individual) and the external auditors' review process demonstrate target-achievement discipline (PT KAI, 2024a).
   In terms of transparency, the KIP/PPID policy, complete with SOPs, implementing units, and the PPID application, demonstrates clear channels of transparency (PT KAI, 2024a).
2. Risk. The ISO 31000 stages (communication–context–identification–analysis–evaluation–treatment–monitoring and review–recording/reporting) are explicitly stated; SMARTKA (go-live 2021) is used by the corporation and 6 subsidiaries for RCSA, indicating process and data integration (PT KAI, 2024a).
3. Compliance. The WBS has defined roles/tasks (reviewer, verifier, admin, investigation), equipped with follow-up and socialization flows, supporting a traceable non-compliance process (PT KAI, 2024a).

Compared to the literature, these results are in line with the OCEG v3.5 idea of reconnecting roles/processes for Principled Performance (OCEG, 2024), but differs from two case studies in Europe/the Netherlands (utility companies and financial institutions) because PT KAI demonstrates a more explicit public transparency channel (PPID mobile app) and a broader digital risk footprint to its subsidiaries (Shahim et al., 2012; PT KAI, 2024a).

This pattern indicates that formal institutional structures are largely in place; however, their operational consolidation across functions and subsidiaries remains uneven, positioning PT KAI predominantly within an intermediate maturity zone rather than a fully optimized GRC state.

Key evidence and maturity implications

Key evidence and maturity implications for each domain are summarized, audit-traceable, and mapped to OCEG practices as follows:

Governance

Strong evidence in the governance domain is evident from the existence of Director KPIs that are set and reviewed periodically, including review by external auditors, strengthening of information disclosure through PPID policies, SOPs, and service applications, as well as statements on the adequacy and effectiveness of the Internal Control System. This combination supports G7 (KPIs), G8 (Reporting), and G11 (Transparency), whose maturity level indicates Levels 3 to 4 (available within the organization, but still scattered/used inconsistently throughout the organization). This intermediate maturity reflects a governance configuration in which accountability mechanisms are formalized, yet cross-entity coordination and feedback loops have not fully converged, limiting the transition toward enterprise-wide continuous improvement and performance learning required at Level 5 (Table 1).

Table 1. OCEG Practices (Governance) and Key Evidence Mapping of PT KAI

OCEG Code and Practices (Governance)	Key Evidence PT KAI (2024)
G1 (Code of Conduct)	Code of Conduct/Ethics, including conflict of interest policies, anti-gratification, WBS; regular communication/training conducted.
G2 (Strategy)	Risk management is integrated into RJPP/RKAP planning as the basis for strategic decisions, an ISO 31000-based framework.
G3 (Organizational Chart)	The governance structure separates the main bodies (GMS/BOC/BOD) and supporting bodies (Audit Committee, Corporate Secretary, etc.).
G4 (Accountabilities)	Application of the Three Lines Model for accountability roles; the Internal Control System (ICS) statement affirms the role of the BOD/BOC in

OCEG Code and Practices (Governance)	Key Evidence PT KAI (2024)
	control effectiveness.
G5 (Meetings between accountable parties)	The Inspectorate/Internal Audit coordinates and holds regular meetings with the Board of Commissioners/Audit Committee and management.
G6 (Process integration with business process)	The GRC process is connected to core processes—SMARTKA/ERM (Enterprise Risk Management), integration into the preparation of RKAP/RJPP, and the digitization of operational processes.
G7 (KPIs)	Board KPIs (collegial and individual) cover safety, timeliness, finance, ESG (Environmental Risk Governance), and risk indicators; there is a summary of achievements.
G8 (Reporting)	Performance reporting/KPIs with targets and actuals; adequate/effective ICS statements are presented in the Annual/Sustainability Report.
G9 (Budget)	Budgeting through the Annual Work Plan and Budget (RKAP) and monitoring of budget/investment absorption as a KPI; the budgeting process related to risk management.
G10 (Cost/benefit monitoring)	Cost monitoring through expense items (e.g., education and training, IT, meetings) is linked to KPI achievements (benefits/performance).
G11 (Transparency)	PPID with policies, SOPs, units, and service channels; PPID application is available for public information services.
G12 (Training)	Anti-corruption and SMAP (Anti-Bribery Management System) ISO 37001, GCG (Good Corporate Governance) training/socialization programs, as well as other training programs (CGRCP, ISO 27001, Risk Management, Safety Leadership).

Risk

Explicit implementation of the ISO 31000 cycle, supported by the digitization of risk management through SMARTKA–RCSA, which has gone live and been adopted by subsidiaries, as well as the integration of safety aspects (HIRADC/IBPR) into SMARTKA and the link between risk management and RKAP/ RJPP objectives. This indicates that practices R1 (Risk Assessment), R2 (Risk Overview including IT), and R4 (Risk Review) have reached a maturity level of 3–4, reflecting partial institutionalization that remains constrained by the coexistence of centralized risk policies and decentralized operational autonomy across units and subsidiaries, while strengthening towards Level 5 requires standardization of root cause analysis, periodic testing of emergency processes, and system log-based leading indicators to ensure measurable continuous improvement (Table 2). The persistence of fragmentation suggests that risk management functions have matured faster at the policy and system level than at the level of routine managerial decision-making and cross-functional integration.

Table 2. OCEG (Risk) Practices and Key Evidence Mapping of PT KAI

OCEG (Risk) Code and Practices	Key Evidence KAI 2024
R1 (Risk Assessment)	The MR process refers to ISO 31000; RCSA is digitized in SMARTKA for all units and subsidiaries; real-time notifications and dashboards accelerate

OCEG (Risk) Code and Practices	Key Evidence KAI 2024
	risk data consolidation.
R2 (Risk overview)	Enterprise risk overview available via SMARTKA (standardization, transaction documentation, KAI Group risk monitoring).
R3 (Risk overview includes IT risks)	IT risk management is proven through the implementation of ISMS ISO 27001 (surveillance audit in May 2024) and annual IT maturity assessments based on COBIT; the IT Masterplan guides business-IT alignment.
R4 (Risk review)	Regular reviews are evident from the 2024 SMKP (Railway Safety Management System) internal/external audit and evaluation of accident causes to prevent recurrence; IT maturity assessments are conducted annually.
R5 (Incident reporting)	Hazard and safety incident reporting through the SRI (Safety Railway Information) application; hazard investigation and identification (IBPR) processes are ongoing.
R6 (Emergency process for gaps and incidents)	The Central Safety Committee assesses emergency response facilities and coordinates disaster management with relevant agencies.
R7 (Root cause analysis (RCA) for gaps/incidents)	Investigations of KKA (train accidents) and NKKA (non-train accidents) aim to find root causes; the ORILIO (Organizational Influences, Operational Risk Control, Local Factors, Individual Actions, Occurrence Events) and SCAT (Systematic Cause Analysis Techniques) methods are used, followed by monitoring of follow-up actions; the RCA special meeting agenda is recorded.

Meanwhile, EY consultant have conducted a 2024 Risk Maturity Index assessment at PT KAI in accordance with five dimensions, namely (i) risk culture and capabilities, (ii) risk organization and governance, (iii) risk and compliance framework, (iv) risk processes and controls, (v) models, data, and technology, based on the Decree of the Deputy for Finance and Risk Management of the Ministry of State-Owned Enterprises of the Republic of Indonesia Number SK-8/DKU.MBU/12/2023 concerning Technical Guidelines for Assessing the Risk Maturity Index within State-Owned Enterprises (BUMN), it can be concluded that the Risk Maturity Index (RMI) of PT KAI (Persero) is 3.04 (EY, 2025). This means that the maturity level indicates Level 3 to 4 (available within the organization, but still scattered/used inconsistently throughout the organization). This external assessment reinforces the documentary findings and suggests that the observed maturity plateau is structurally stable rather than a temporary transition phase.

Compliance

The compliance architecture is supported by conflict of interest and anti- corruption policies, the implementation of SMAP ISO 37001 with surveillance results showing no findings (0 major, 0 minor, 0 OBS, 14 OFI), updates to guidelines and WBS applications integrated with the KPK through a cooperation agreement, as well as disciplined LHKPN reporting and the signing of a Code of Ethics that is almost universal; all of this evidence indicates a maturity level of Level 3 to 4 (available within the organization, but still scattered/used inconsistently throughout the organization) on C1–C4. This relatively consistent compliance maturity is largely driven by regulatory mandates and external oversight, which promote uniform adoption but also introduce

rigidity that may limit adaptive integration with risk and performance management, while to reach Level 5, it is necessary to expand the scope of certification/implementation to high- risk processes (e.g., end-to-end procurement), establish investigation SLAs and publish misconduct handling performance metrics, and strengthen compliance-by-design in core systems (Table 3).

Table 3. OCEG (Compliance) Practices and Key Evidence Mapping of PT KAI

OCEG (Compliance) Codes and Practices	**Key Evidence PT KAI 2024**
C1 (Overview of regulatory boundaries)	The main obligation framework referred to includes POJK 51/2017, SE OJK 16/2021, GRI 2021, SDGs in sustainability reporting; the KIP regime is implemented through PPID (policy/SOP/organization) as an information service obligation; integration of TPK handling through the KAI–KPK Cooperation Agreement (PKS) and e-Gratification governance in accordance with KPK Regulation 2/2019.
C2 (Overview of internal and external rules and regulations)	Code of Conduct/Code of Ethics and Board of Directors conflict of interest policy (declaration, integrity pact, prohibition of self-dealing/insider information); anti-corruption and gratification policies; WBS guidelines/SOPs updated on January 12, 2024 (PER.U/KL.104/1/KA-2024); SMAP ISO 37001 framework as an external reference standard.
C3 (Compliance review)	External surveillance of ISO 37001:2024 with results of 0 major, 0 minor, 0 OBS, 14 OFI; LHKPN achieved 100% (1,215 reporters) as an indicator of compliance discipline; the Board of Commissioners supervises the implementation of WBS.
C4 (Processes when confronted with non-compliance)	WBS provides an intake–triage–verification–investigation–sanction process with clear roles (reviewer, verifier, admin, investigation team); case data is available (2024: 23 reports, 2 proven and followed up), as well as disciplinary sanctions; the KAI–KPK Cooperation Agreement allows for the referral/exchange of data on corruption cases to prevent duplication of handling.

Strategic alignment and differences with previous research

The evidence mapping results show the relationship between GRC and RJPP/RKAP, as well as risk digitization through SMARTKA. This is consistent with the SAM framework that success depends on the fit between strategy, process, and solution (Shahim et al., 2012). In the context of KAI, the implementation pattern is close to Path B (Technology Transformation), where the GRC strategy is derived from the business strategy, then accommodated by IT solutions and embedded into processes—with elements of Path D (Service Level) when the solution is integrated into the performance assessment infrastructure (KPI/ICS) (Shahim et al., 2012; PT KAI, 2024a) (Figure 3).

Figure 3. Vision, Mission, and Roadmap Information Technology PT KAI

This alignment choice implies a predominantly top-down transformation logic, in which technology serves as an enabler of strategic intent, but may constrain bottom-up learning and cross-functional experimentation.

Unlike case studies of utility companies and financial institutions in Europe/the Netherlands (Shahim et al., 2012) that emphasize the path-dependency of existing IT assets, PT KAI adds the factor of public transparency (PPID) as a strong governance variable in the Indonesian public service sector (PT KAI, 2024a).

Discussion of differences with previous publications

PT KAI's results show a combination of solution-based alignment (SMARTKA) and strengthening public governance (PPID, KPI, ICS). Previous studies emphasized path variation due to IT assets (Shahim et al., 2012), while at PT KAI, the regulatory transparency framework (KIP/PPID) and sustainability reporting that refers to GRI–POJK strengthen the governance pillar illustrating how public-sector accountability requirements shape a distinct alignment trade-off, where transparency and compliance maturity advance more rapidly than integrated risk-informed strategic coherence (PT KAI, 2024a).

CONCLUSION

This study targets three objectives: (i) formulating an assessment framework of 23 OCEG-based GRC practices for the context of PT KAI; (ii) mapping evidence from 2024 documents (Annual and Sustainability Reports, Company Profile, and Financial Statements) to each practice so that it is traceable; and (iii) presenting an indicative maturity assessment and strategic alignment implications (A–D) in the style of the Strategic Alignment Model (SAM). All three objectives were met. First, the 23 practice instruments (12–7–4; scale 1–5) were adopted from the literature and standardized for replication. Second, evidence mapping shows clear evidence in the domains of governance (Board KPI and external review), risk (ISO 31000 and SMARTKA–RCSA stages), and compliance (WBS design and handling flow) that can be traced back to documents (PT KAI, 2024a).

Third, the synthesis results show that the most "fit" alignment pattern for KAI tends to be close to Path B (Technology Transformation)—the GRC strategy is derived from the corporate strategy, then accommodated by IT solutions and embedded into the process with elements of Path D (Service Level) when the solution is integrated into the performance infrastructure (KPI/ICS) (Shahim et al., 2012; PT KAI, 2024a).

Indicatively, the maturity of KAI's GRC in 2024 is concentrated at Levels 3 to 4 (available within the organization, but still scattered/used inconsistently across the organization) for some governance practices (KPI/reporting, transparency/PPID) and risk (digitalized ISO 31000-based assessment and review), while several other practices are at Level 3 (available but not yet evenly distributed across entities) (PT KAI, 2024a). This assessment is in line with the OCEG v3.5 thesis that GRC is an integrated capability that "reconnects" roles/processes for Principled Performance (OCEG, 2024), while expanding on the findings of case studies in Europe/the Netherlands (utility companies and financial institutions) by adding the nuance of the public sector: the existence of PPID transparency channels and digital risk footprints that reach subsidiaries (Shahim et al., 2012; PT KAI, 2024a).

Contribution to the development of science/practice

This study (i) offers a replication protocol for GRC maturity assessment based on 23 practices and detailed evidence mapping; (ii) shows how to read the alignment trajectory (A–D) from real organizational evidence—not normative assumptions—so that implementation strategy choices (e.g., focusing on technology transformation first) have an empirical basis; and (iii) integrates Lines of Accountability and the OCEG v3.5 total performance paradigm into the GRC alignment discourse, enriching the literature that previously emphasized asset-driven alignment pathways (OCEG, 2024; Shahim et al., 2012).

LIMITATIONS AND FURTHER RESEARCH

Limitations

This study relies on PT KAI's 2024 documentary evidence (Annual and Sustainability Report, Company Profile, Financial Statements), so it is cross-sectional in nature and does not capture cross-year dynamics or delayed implementation effects. Reliance on corporate documents also carries the potential for reporting bias (e.g., selection of information emphasized in governance/sustainability narratives), so caution is needed when interpreting findings, especially regarding the effectiveness of processes (PT KAI, 2024a, 2024b, 2024c).

Second, there were no direct interviews/observations of key stakeholders (e.g., risk owners, Internal Audit, Board Committee), so that real working mechanisms, such as the frequency of cross-three-lines challenges or the quality of risk discussions, were inferred from policies, structures, and reporting, rather than from actual behavior (PT KAI, 2024a).

Third, although evidence of the ISO 31000 framework and SMARTKA/RCSA digitization is available, this study has not conducted process mining/audit log analytics on system data to assess process conformance and throughput (PT KAI, 2024a). As a result, the maturity scores presented are indicative and rely on documentary evidence; construct validity has been maintained through strict mapping, but the internal validity of process performance has not been computationally tested.

Fourth, the generalization is still limited. The single-case design at the Indonesian railway SOE (PT KAI) is within a unique regulatory regime and public service mandate; therefore, extrapolation to other sectors/countries requires separate evidence (Shahim et al., 2012).

Further Research

1. Methodological triangulation. Complement documentary analysis with semi-structured interviews (BoD/BoC, Audit/Risk Monitoring Committee, risk owners, IA), process mining of SMARTKA/RCSA logs to test conformance and lead time, and observation of cross-three-lines meetings to capture micro-governance in practice (PT KAI, 2024a).
2. Longitudinal and cross-case validation. Build a multi-year (≥3 years) and multi-case (other railway operators or subsidiaries) panel to test the stability of maturity scores and alignment trajectories (A–D) within the SAM framework (Shahim et al., 2012).

ETHICS, FUNDING, CONFLICT OF INTEREST STATEMENT, AND DATA AVAILABILITY

This study only uses publicly available secondary documents (2024 Annual & Sustainability Report, 2024 Company Profile, and 2024 Financial Report of PT KAI) without involving human/animal subjects, thus not requiring ethical committee approval in accordance with general guidelines for document-based research; if the publishing institution requires it, the author is prepared to provide an ethics exemption statement from the institution of origin.

Funding

This research did not receive specific funding from public, commercial, or non- profit funding agencies; all costs were borne by the author.

Conflict of interest statement

The authors have no conflicts of interest that could influence the design, analysis, or reporting of the results of this study.

Data availability

All primary data sources are public and accessible through PT KAI's official 2024 publication; the 23 practice instruments, evidence mapping templates, and "evidenceregister" summary (without confidential information/PII (Personally Identifiable Information) are provided as Supplementary Material and/or are available upon reasonable request to the authors; data that may contain company confidentiality or privacy protections cannot be distributed.

REFERENCES

Abdurrahman, A., Gustomo, A., & Prasetio, E. (2023). Enhancing banking performance through dynamic digital transformation capabilities and governance, risk management, and compliance: Insights from the Indonesian context. *The Electronic Journal of Information Systems in Developing Countries, 90*(2), Article e12299. https://doi.org/10.1002/isd2.12299

Adama, H., Popoola, O., Okeke, C., & Akinoso, A. (2024). Theoretical frameworks supporting IT and business strategy alignment for sustained competitive advantage. *International Journal of Management & Entrepreneurship Research, 6*(4), 1273–1287. https://doi.org/10.51594/ijmer.v6i4.1058

Alves, L., Gomes, C., Silva, F., Santos, M., & Lucas, S. (2023). Proposal of a new multicriteria methodology Sapevo-Waspas-2N applied in prioritizing the implementation of compliance processes. *Operations Research Perspectives, 10*, 100272. https://doi.org/10.1016/j.orp.2023.100272

Attalansyah, A., & Anshori, M. (2023). Adaptive policy education in the VUCA era for Jetis Sidoarjo batik craftsmen. *Journal of Business Management and Economic Development, 2*(1), 323–336. https://doi.org/10.59653/jbmed.v2i01.494

Bantleon, U., d'Arcy, A., Eulerich, M., Hucke, A., Pedell, B., & Ratzinger-Sakel, N. V. S. (2021). Coordination challenges in implementing the three lines of defense model. *International Journal of Auditing, 25*(1), 59–74. https://doi.org/10.1111/ijau.12201

Banke, M., Lenger, S. F., & Pott, C. (2022). ESG ratings in the corporate reporting of DAX40 companies in Germany: Effects on market participants. *Sustainability, 14*(15), Article 9742. https://doi.org/10.3390/su14159742

Beasley, M. S., Branson, B. C., Braumann, E., & Pagach, D. (2023). Understanding the ecosystem of enterprise risk governance. *The Accounting Review, 98*(5), 99–125. https://doi.org/10.2308/TAR-2020-0488

Bouteska, A., & Mili, M. (2022). Does corporate governance affect financial analysts' stock recommendations, target prices accuracy and earnings forecast characteristics? *Empirical Economics, 63*(4), 2125–2171. https://doi.org/10.1007/s00181-022-02297-3

Ernst & Young. (2025). *Results of the risk maturity index assessment of PT Kereta Api Indonesia for 2024* [Unpublished internal report].

Fisher, L., & Sandberg, A. (2022). A safe governance space for humanity: Necessary conditions for the governance of global catastrophic risks. *Global Policy, 13*(5), 792–807. https://doi.org/10.1111/1758-5899.13030

Garcia-Lacalle, J., & Torres, L. (2021). Financial reporting quality and online disclosure practices in Spanish governmental agencies. *Sustainability, 13*(5), Article 2437. https://doi.org/10.3390/su13052437

Gerwing, T., Kajüter, P., & Wirth, M. (2022). The role of sustainable corporate governance in mandatory sustainability reporting quality. *Journal of Business Economics, 92*(3), 517–555. https://doi.org/10.1007/s11573-022-01092-x

Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal, 32*(1), 4–16. https://doi.org/10.1147/sj.382.0472

Imgharene, K., Baïna, S., & Doumi, K. (2019). Extending the strategic alignment model: A synchronization perspective. In *Proceedings of the International Conference on Information Systems*. https://doi.org/10.33965/is2019_201905l019

Katz, B., Louw, L., & du Preez, N. (2016). Alignment of internal and external business and innovation domains. *South African Journal of Industrial Engineering, 27*(1), 1–14. https://doi.org/10.7166/27-1-1247

Kurniawan, K., Sugandi, Y., Widianingsih, I., & Nurasa, H. (2024). Governance, risks, and compliance in fulfilling the new and renewable energy mix at the state electricity company (PLN). *Journal of Ecohumanism, 3*(8), Article 4749. https://doi.org/10.62754/joe.v3i8.4749

Makaš, A. (2023). Governance, risk and compliance frameworks applicability in organizations. *International Journal of Science and Research Archive, 10*(2), 716–724. https://doi.org/10.30574/ijsra.2023.10.2.1024

OCEG. (2024). *GRC capability model™ (Version 3.5; Revision 2024-01-22)*. https://www.oceg.org/grc-capability-model-red-book/

Omotayo, T., Awuzie, B., Kenechukwu, V., Ajayi, S., Obi, L., Osobajo, O., & Oke, A. (2022). System dynamics analysis of cost overrun causations in UK rail projects in a COVID-19 epidemic era. *SAGE Open, 12*(2), Article 21582440221097923. https://doi.org/10.1177/21582440221097923

PT Kereta Api Indonesia (Persero). (2024a). *Annual and sustainability report 2024*. https://www.kai.id/hubungan_investor/laporan/

PT Kereta Api Indonesia (Persero). (2024b). *Company profile 2024*. https://www.kai.id/corporate/about_kai/

PT Kereta Api Indonesia (Persero) & Subsidiaries. (2024c). *Consolidated financial statements 2024 (audited)*. https://www.kai.id/hubungan_investor/laporan/

Rehman, H., Ramzan, M., Haq, M. Z. U., Hwang, J., & Kim, K.-B. (2021). Risk management in corporate governance framework. *Sustainability, 13*(9), Article 5015. https://doi.org/10.3390/su13095015

Sabherwal, R., Sabherwal, S., Havakhor, T., & Steelman, Z. (2019). How does strategic alignment affect firm performance? *MIS Quarterly, 43*(2), 453–474. https://doi.org/10.25300/misq/2019/13626

Sardana, D., Terziovski, M., & Gupta, N. (2016). The impact of strategic alignment and responsiveness to market on manufacturing firm performance. *International Journal of Production Economics, 177*, 131–138. https://doi.org/10.1016/j.ijpe.2016.04.018

Shahim, A., Batenburg, R., & Vermunt, G. (2012). Governance, risk and compliance: A strategic alignment perspective applied to two case studies. In *ICT critical infrastructures and society* (IFIP Advances in Information and Communication Technology, Vol. 386, pp. 202–212). Springer. https://doi.org/10.1007/978-3-642-33284-5_20

Siahaan, M., Suharman, H., Fitrijanti, T., & Umar, H. (2022). Will the integrated GRC implementation be effective against corruption? *Journal of Financial Crime, 30*(1), 24–34. https://doi.org/10.1108/JFC-12-2021-0275

Tejada-Malaspina, M., & Jan, A. (2019). An intangible-asset approach to strategic business–IT alignment. *Systems, 7*(1), Article 17. https://doi.org/10.3390/systems7010017

Vicente, P., & Silva, M. (2011). A conceptual model for integrated governance, risk and compliance. In *Governance, risk and compliance handbook* (pp. 199–213). Springer. https://doi.org/10.1007/978-3-642-21640-4_16

Wahyuningrum, I. F. S., Chegenizadeh, A., Humaira, N. G., Budihardjo, M. A., & Nikraz, H. (2023). Corporate governance research in Asian countries: A bibliometric and content analysis (2001–2021). *Sustainability, 15*(8), Article 6381. https://doi.org/10.3390/su15086381

Wiesche, M., Berwing, C., Schermann, M., & Krcmar, H. (2011). Patterns for understanding control requirements for information systems for governance, risk management, and compliance. In *Enterprise information systems* (pp. 208–217). Springer. https://doi.org/10.1007/978-3-642-22056-2_23